REMARKS

In view of the following discussion, the Applicants submit that none of the claims now pending in the application are anticipated or obvious under the provisions of 35 U.S.C. §§ 102 and 103. Thus, the Applicants believe that all of these claims are now in allowable form.

I. AMENDMENT TO THE SPECIFICATION

The Examiner has objected to the specification because the abstract of the disclosure is not clearly defined as "Abstract". The Applicants respectfully submit that the original application as filed clearly defined the abstract as "ABSTRACT OF THE DISCLOSURE". Moreover, no subsequent response or amendment was made to remove the heading. Regardless, the Applicants herein amend the previously presented paragraph [0018] with the heading "ABSTRACT OF THE DISCLOSURE" as required by 37 CFR 1.72(b). As such, the Applicants respectfully request the objection be withdrawn.

II. REJECTION OF CLAIMS 1-4 AND 6-11 UNDER 35 U.S.C. § 102

The Examiner has rejected claims 1-4 and 6-11 in the Office Action under 35 U.S.C. § 102 as being anticipated by Jones, et al. (US Patent 5,623,637, Issued April 22, 1997, hereinafter referred to as "Jones"). The Applicants note that the Examiner states in the Office Action that claims 1-11 are rejected under 35 U.S.C. 102; however, claim 5 is not listed under section 6 of the 35 U.S.C. 102 rejection in the Office Action, but rather under section 8 as being rejected under 35 U.S.C. 103. The Applicants will assume that Examiner meant to only reject claims 1-4 and 6-11 under 35 U.S.C. 102 and proceed under that assumption. Regardless, the Applicants respectfully traverse the rejection.

Jones teaches an encrypted data storage card including smartcard integrated circuit for storing an access password and encryption keys. A user in possession of the card enters a password stored in the card's memory. (See Jones, col. 8, ll. 47-67.) If the password is correct, the user has access to needed access codes stored in the password-protected card. (See Jones, col. 9, ll. 1-21.)

PAGE 8/12 * RCVD AT 5/15/2006 11:55:55 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):03-48

The Examiner's attention is directed to the fact that Jones fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10. Specifically, Applicants' independent claims 1 and 10 recite:

> 1. A security mechanism for enabling a user to commence a session between a network peripheral device and a network, comprising:
> an immutable memory element that contains first information including application software that initiates and provides security services;
> a persistent memory element that contains second information to enable the security mechanism to configure the network peripheral device to access different networks;
> a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session; and
> a tamper-evident enclosure for enclosing the memory elements.
> (Emphasis Added)

> 10. A method for facilitating a secure connection session with a user between a network peripheral device and a network, comprising the steps of:
> accessing an immutable memory element that contains first information that provides security services;
> accessing a persistent memory element that contains second information including configuration information to enable the security mechanism to configure the network peripheral device to access a network;
> accessing a volatile memory element that contains third information, including the critical data for authentication; and
> erasing said third information not later than the end of the connection session so no third information remains in the volatile memory between sessions.
> (Emphasis Added)

Applicants' invention teaches the novel concept of a security mechanism for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session. Applicants' invention

PAGE 9/12 * RCVD AT 5/15/2006 11:55:55 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):03-48

advantageously allows a device to be configured to access any network and the corresponding network's software (see Applicants' Specification, para. [0006]; para. [0013]). In other words, the same laptop, for example, can be connected to various networks. Once the session is completed all of the information in the volatile memory element is erased, thereby preventing re-use of such information by unauthorized users. (See Applicants' Specification, para. [0006].)

In contrast Jones fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10. In fact, Jones teaches away from the Applicants' invention because Jones clearly teaches that critical information is stored in the card's memory and fails to teach that this information is erased from the volatile memory at the completion of each connection session. (See Jones, col. 8, ll. 47-67; col. 9, ll. 1-21.) Jones specifically teaches that a user supplies a secret password that is written into the smart card I.C. memory. (See Jones, col. 8, ll. 6-9, emphasis added.) Jones further teaches that ". . . whose processor (i.e. the smart card) is programmed to combine the random number 303 at 325 with the previously stored secret password 301 to form a result value at 327." (See Jones, col. 8, ll. 21-24, emphasis added.) Therefore, Jones clearly fails to anticipate Applicants' invention as recited in independent claims 1 and 10.

Moreover, dependent claims 2-4, 6-9 and 11 depend, either directly or indirectly, from independent claims 1 and 10, respectively, and recite additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claims 2-4, 6-9 and 11 are also not anticipated by Jones. As such, the Applicants respectfully request the rejection be withdrawn.

III. REJECTION OF CLAIM 5 UNDER 35 U.S.C. § 103

The Examiner has rejected claim 5 in the Office Action under 35 U.S.C. § 103 as being unpatentable over Jones in view of Official Notice. Applicants respectfully

PAGE 10/12 * RCVD AT 5/15/2006 11:55:55 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):03-48

traverse the rejection.

The teachings of Jones are discussed above. As stated above, the Examiner's attention is directed to the fact that Jones fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10 (see *supra*).

Applicants' invention teaches the novel concept of a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session. Applicants' invention advantageously allows a device to be configured to access any network and the corresponding network's software (see Applicants' Specification, para. [0006]; para. [0013]). In other words, the same laptop, for example, can be connected to various networks. Once the session is completed all of the information in the volatile memory element is erased, thereby preventing re-use of such information by unauthorized users. (See Applicants' Specification, para. [0006].)

As discussed above, Jones fails to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10. In fact, Jones teaches away from the Applicants' invention because Jones clearly teaches that critical information is stored in the card's memory and fails to teach that this information is erased from the volatile memory at the completion of each connection session. (See Jones, col. 8, ll. 47-67; col. 9, ll. 1-21.) Moreover, the Examiner's Official Notice fails to bridge the substantial gap left by Jones. Even if the Examiner's Official Notice and Jones were combined, the combination would only teach critical information that is stored in write-

PAGE 11/12 * RCVD AT 5/15/2006 11:55:55 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):03-48

once ROM memory. The combination would still fail to teach, show or suggest a security mechanism or method for enabling a user to commence a session between a network peripheral device and a network comprising a volatile memory element that contains third information, including the critical data for authentication, said third information erased from the volatile memory at the completion of each connection session, as positively claimed by Applicants' independent claims 1 and 10.

Moreover, dependent claim 5 depends indirectly from independent claim 1 and recites additional limitations. As such, and for the exact same reason set forth above, the Applicants submit that claim 5 is also not made obvious by the teachings of Jones in view of the Examiner's Official Notice. As such, the Applicants respectfully request the rejection be withdrawn.

Conclusion

Thus, the Applicants submit that all of these claims now fully satisfy the requirements of 35 U.S.C. §§ 102 and 103. Consequently, the Applicants believe that all these claims are presently in condition for allowance. Accordingly, both reconsideration of this application and its swift passage to issue are earnestly solicited.

If, however, the Examiner believes that there are any unresolved issues requiring the issuance of a final action in any of the claims now pending in the application, it is requested that the Examiner telephone Mr. Kin-Wah Tong, Esq. at (732) 530-9404 so that appropriate arrangements can be made for resolving such issues as expeditiously as possible.

Respectfully submitted,

5/15/06

Patterson & Sheridan, LLP
595 Shrewsbury Avenue
Shrewsbury, New Jersey 07702

Kin-Wah Tong, Attorney
Reg. No. 39,400
(732) 530-9404

PAGE 12/12 * RCVD AT 5/15/2006 11:55:55 PM [Eastern Daylight Time] * SVR:USPTO-EFXRF-1/0 * DNIS:2738300 * CSID:732 530 9808 * DURATION (mm-ss):03-48